RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 471 003**
(A n'utiliser que pour les commandes de reproduction).

A1

DEMANDE DE BREVET D'INVENTION

(21) **N° 79 29585**

(54) **Système à objet portatif présentant une information confidentielle et lecteur de cette information, notamment pour des transactions financières et/ou commerciales.**

(51) Classification internationale (Int. Cl. ³). G 06 K 19/00, 7/08; H 03 K 13/00.

(22) Date de dépôt ..... 30 novembre 1979.

(33) (32) (31) Priorité revendiquée :

(41) Date de la mise à la disposition du public de la demande ..... B.O.P.I. — « Listes » n° 24 du 12-6-1981.

(71) Déposant : Société dite : ELECTRONIQUE MARCEL DASSAULT, résidant en France.

(72) Invention de : Jean-Claude Basset.

(73) Titulaire : *Idem* (71)

(74) Mandataire : André Netter, conseil en brevets d'invention, 40, rue Vignon, 75009 Paris.

2471003

L'invention est relative à un système à objet portatif présentant des informations confidentielles, par exemple une carte de crédit ou un ticket d'accès aux transports en commun ou analogue, et lecteur de telles informations permettant de déclencher une opération si l'information correspond à une autorisation.

Dans le cas d'une carte de crédit ou d'achat, l'opération est une transaction financière et/ou commerciale, qui est effectuée après comparaison entre l'information confidentielle portée par la carte et le numéro ou autre information tapé par le titulaire sur un clavier associé au lecteur. Dans le cas d'un ticket d'accès, c'est la conformité de l'information portée par ce ticket avec une information en mémoire qui autorise l'accès.

De telles cartes ou tickets comprennent généralement une ou plusieurs pistes magnétiques sur lesquelles sont inscrites les données confidentielles. Mais ces données peuvent être lues avec un équipement relativement simple, ce qui entraîne un risque de fraude non négligeable. La densité par unité de surface des informations que peut contenir une piste magnétique ne pouvant dépasser des valeurs relativement modestes, une telle piste ne peut stocker qu'une quantité limitée d'informations. Pour cette raison, si le lecteur n'est pas connecté à un calculateur central, les cartes de crédit ou d'achat de ce type ne sont utilisées que pour commander des opérations relativement simples.

On a déjà proposé, pour diminuer les risques de fraude et pour élargir les possibilités d'utilisation d'objets portatifs de remplacer les pistes magnétiques par des circuits électroniques intégrés. Mais les risques de fraude sont encore importants avec les objets portatifs connus de ce genre.

L'invention remédie à cet inconvénient. Elle rend particulièrement difficile l'utilisation frauduleuse d'un objet portatif à circuits électroniques intégrés présentant des informations confidentielles.

Elle part de la constatation que l'analyse des signaux échangés entre les circuits de l'objet et ceux du lecteur, en vue d'une utilisation frauduleuse, ne peut être effectuée

qu'à l'aide d'un calculateur programmé tel qu'un microprocesseur.

Le système selon l'invention est caractérisé en ce que les circuits intégrés de l'objet et du lecteur sont spécifiques, non programmables, de façon que la durée d'échange des signaux entre les circuits de l'objet et ceux du lecteur soit réduite à un minimum et en ce que des moyens sont prévus pour empêcher que se réalise l'opération que doit commander l'introduction de l'objet portatif dans le lecteur, si cette durée dépasse une limite prédéterminée.

De cette manière, si un microprocesseur est connecté à la liaison entre l'objet et le lecteur, il ne disposera pas, même si sa programmation est optimisée, d'un temps suffisant pour analyser les signaux échangés entre l'objet et le lecteur car sa vitesse de calcul est nécessairement plus faible que la vitesse de l'échange des signaux entre circuits conçus spécifiquement pour un tel échange.

Dans une réalisation, on prévoit dans l'objet portatif et/ou dans le lecteur, des moyens pour déterminer si chaque message reçu de l'autre partie du système a une structure ou composition convenable, eu égard à une multiplicité de critères tels que le format, notamment la longueur du message, la parité et le code de la fonction, des moyens pour demander une répétition de ce message dans le cas contraire, et un compteur des demandes de répétition, empêchant que s'effectue par la suite l'opération déclenchable par l'introduction de l'objet dans le lecteur, quand le nombre de répétitions dépasse une limite prédéterminée, de préférence inférieur au nombre de messages nécessaires pour commander ladite opération. Ce nombre de demandes de répétition autorisé sera cependant, de préférence, au moins égal à deux, de façon qu'une erreur de transmission due, par exemple, à des parasites ou à l'encrassement des contacts de l'objet, ne provoque une interdiction intempestive. Le compteur du nombre de demandes de répétition est ainsi un détecteur de tentative de fraude dont le signal peut être utilisé pour empêcher toute utilisation ultérieure de l'objet, par exemple par destruction d'un fusible d'un circuit de cet objet.

Selon une autre disposition de l'invention, qui a également pour but de réduire les risques d'utilisation frauduleuse d'un objet portatif présentant des informations confidentielles, ces dernières sont, dans ledit objet, codées de telle manière que les signaux sortant de cet objet et traduisant ces informations vers le lecteur ne soient pas identiques aux informations connues par le titulaire de l'objet, des moyens étant prévus pour que le code soit transmis au lecteur.

La fraude est rendue encore plus difficile si le codage de l'information confidentielle est effectué à l'aide d'un code choisi au hasard, lors de l'introduction de l'objet dans le lecteur, parmi un nombre important ou une infinité de codes.

Les messages émis par le lecteur en direction des circuits de l'objet peuvent être également codés, des moyens étant prévus pour transmettre le code audit objet. Dans ce cas, il est aussi possible de choisir de façon aléatoire ou quasi-aléatoire le code lors de la connexion de l'objet.

La réalisation des circuits peut être facilitée si le codage est du type polynomial, c'est-à-dire que, si le nombre binaire X à coder a pour valeur :

$$X = x_n\, x_{n-1} \cdots x_2 x_1 x_o \ ,$$

le nombre binaire codé sera une combinaison de chiffres binaires X_p :

$$X_p = a_o^p\, x_o + a_1^p\, x_1 + \ldots + a_n^p\, x_n$$

Dans cette formule, les coefficients $a_o^p \ldots a_n^p$ sont des chiffres binaires représentatifs du codage.

D'autres caractéristiques de l'invention apparaîtront avec la description de certains de ses modes de réalisation, celle-ci étant effectuée en se référant aux dessins ci-annexés, sur lesquels :

la figure 1 montre de façon très schématique la structure générale d'un système à carte à circuit électronique intégré et lecteur de cartes;

la figure 2 est un schéma d'un circuit de demande de répétitions;

la figure 3 représente un circuit de codage;

la figure 4 est un schéma d'un circuit du lecteur;

la figure 5 est un schéma d'un circuit d'une carte;et

la figure 6 représente la combinaison de deux circuits de codage.

Le système représenté sur la figure 1 se compose d'une carte 10 formée d'un support standard en matière plastique, sur lequel est disposé, par exemple par collage, ou à l'intérieur duquel est(sont) noyée(s) une (ou plusieurs) pastille(s) de circuits électroniques intégrés 11 présentant un certain nombre, cinq dans l'exemple, de bornes 12 à 16 d'entrée-sortie pour leur connexion aux bornes correspondantes 12_1 à 16_1 d'entrée-sortie de circuits 17 se trouvant à l'entrée d'un terminal 18. La connexion entre les bornes des circuits 11 et 17 s'effectue, de façon classique, par simple introduction de la carte 10 dans une fente du terminal 18.

Les circuits 17 sont reliés, par l'intermédiaire d'autres connexions 19 et 20, à des bornes d'entrée-sortie de circuits 21 de gestion et de calcul des opérations à effectuer par le terminal, ces derniers circuits présentant d'autres bornes d'entrée-sortie 22_1 , 23_1 connectées par l'intermédiaire de conducteurs 22 et 23, à un appareil 24 assurant l'opération à réaliser et présentant un clavier 25 sur lequel le titulaire de la carte 10 frappe une information confidentielle qui lui est propre, telle qu'un numéro qu'il est en principe seul à connaître, permettant de vérifier, par la comparaison avec les numéros mémorisés par les circuits 11, que le détenteur de la carte est autorisé à l'utiliser. L'appareil 24, qui se trouve chez un commerçant et n'est pas connecté à un calculateur central, est destiné à écrire sur une carte analogue à la carte 10, des informations de crédit du compte du commerçant, les informations de débit étant alors inscrites dans les circuits 11.

En variante, l'appareil 24 est un distributeur de billets de banque et le terminal 18 est connecté à un calculateur central.

Les signaux transmis par les circuits 11 aux circuits 17 et vice versa sont des signaux série du type informatique. Chacune des lignes de connexion transmet une information d'un

type déterminé; ainsi, sur la ligne H entre les bornes 12 et 12_1 sont transmis les signaux de synchronisation; les bornes 13 et 13_1 sont reliées l'une à l'autre par une ligne E/S transmettant les signaux d'information; la ligne V reliant les bornes 14 et 14_1 transmet l'énergie, à tension déterminée, d'excitation des circuits de la carte 10; la ligne M entre les bornes 15 et 15_1 est portée au potentiel de la masse; et la ligne PR entre les bornes 16 et 16_1 est destinée à transmettre des signaux d'inscription de données dans la mémoire des circuits 11, l'énergie nécessaire à une inscription en mémoire étant en général supérieure à l'énergie nécessaire pour transmettre une simple information.

Dans ce qui suit, pour simplifier l'exposé, l'opération effectuée par l'appareil 24, après autorisation, sera appelée transaction.

Les circuits 17 du terminal 18 et les circuits 11 de la carte 10 sont, selon l'invention, réalisés sous forme de circuits spécifiques, non programmables, de manière que le temps d'exécution des calculs qu'ils sont destinés à effectuer soit réduit à un minimum, inférieur au temps que mettrait, pour effectuer les mêmes calculs, un microprocesseur programmé à cet effet et des moyens sont prévus pour interdire la transaction si la durée de transmission des messages dépasse une limite prédéterminée ou si la vitesse de transmission tombe au-dessous d'un seuil déterminé.

A cet effet, dans la réalisation représentée sur la figure 2, les circuits 17 du terminal 18 et les circuits 11 de la carte 10 comportent chacun un circuit 26 de comptage des demandes de répétition de messages. Ce circuit autorise, au cours de chaque introduction d'une carte dans un terminal, un nombre déterminé N de répétitions de messages envoyés par les circuits 11 vers les circuits 17, ou réciproquement par les circuits 17 vers les circuits 11, afin de tenir compte des erreurs de transmission provoquées par des parasites sur les connexions, notamment la connexion E/S, ou encore par un encrassement de contacts ou une défectuosité temporaire de l'un des éléments des circuits. Par contre, si le nombre N de demandes de répétition de messages est dépassé, un signal

est engendré pour interdire la transaction. L'interdiction peut être temporaire, par exemple par la fermeture d'une porte; elle peut également être définitive, par exemple par l'inscription d'une information correspondante en mémoire des circuits 11, ou encore par destruction d'un fusible dans ces circuits.

Le nombre N est de préférence au moins égal à 2 mais inférieur au nombre de messages nécessaires pour commander la transaction.

Cette disposition empêche que le ralentissement volontaire de la transmission des messages, afin de disposer d'un temps suffisant pour les analyser, par exemple à l'aide d'un microprocesseur et éventuellement d'autres circuits, puisse conduire à la transaction, les erreurs ou parasites n'empêchant cependant pas cette transaction.

A la borne 13, ou 13_1 , est connecté d'une part un codeur 27 présentant une porte de blocage et, d'autre part, un organe 28 de comparaison et de décodage. La sortie 29 de l'organe 28 est reliée à l'entrée 30 d'un registre 31 de réception de messages qui présente une sortie 32 reliée à une entrée 33 d'un registre 34 d'émission de messages qui comporte une autre entrée 35 connectée à la sortie 36 d'un circuit 37 de demandes de répétition, dont l'entrée 38 est reliée à une seconde sortie 39 de l'organe 28 et dont une autre sortie 40 est connectée à l'entrée 41 d'un compteur 42 des demandes de répétition.

La sortie 43 du compteur 42 est reliée à l'entrée 44 du codeur 27 dont une autre entrée 45 est connectée à la sortie du registre 34 d'émission de messages.

Le fonctionnement du circuit 26 est le suivant :

Dans l'organe 28, les messages provenant de la ligne E/S sont décodés et comparés, du point de vue de leur longueur, de leur code fonction et de la détection des erreurs à des informations appliquées à une autre entrée 29a de cet organe 28. Ainsi, on peut déterminer si le message a une composition appropriée dans la séquence des signaux échangés entre les circuits 11 et 17.

Si l'organe 28 ne détecte pas d'erreur, le message reçu

par la ligne E/S est appliqué sur la sortie 29 pour valider le registre 31, alors que dans le cas contraire, c'est-à-dire si la comparaison effectuée par l'organe 28 révèle une erreur, le registre 31 n'est pas validé et il apparaît un signal sur la sortie 39 qui active le circuit 37 de demandes de répétition. La demande de répétition est transmise, par la sortie 36 du circuit 37, au registre 34 d'émission de message et cette demande de répétition, codée par le codeur 27, est transmise, par la ligne E/S, à l'autre partie du système. En même temps, un signal sur la sortie 40 du circuit 37 augmente d'une unité le contenu du compteur 42 de demandes de répétition. Quand ce nombre atteint la valeur N, un signal apparaît sur la sortie 43 qui est appliqué sur l'entrée 44 du codeur bloqueur 27 pour activer la porte de blocage qu'il contient et ainsi interdire la poursuite de l'échange des signaux entre les circuits 11 et 17.

Selon une autre disposition de l'invention, les messages échangés entre les circuits 11 et 17 immédiatement après l'introduction de la carte 10 dans le terminal 18, ont pour but d'initialiser lesdits circuits selon une séquence prédéterminée. Ainsi, des registres, des bascules, des mémoires, des séquenceurs de phase sont positionnés et des calculs sont exécutés, par exemple à l'aide des informations contenues en mémoire des circuits 11. Cette initialisation est complexe et de brève durée afin de constituer un obstacle à la fraude.

Cette phase d'initialisation permet également de vérifier que les circuits 11 et 17 fonctionnent normalement.

Selon encore une autre disposition de l'invention, les messages échangés entre les circuits 11 et les circuits 17 sont codés, pour ceux émanant des circuits 11 par un premier code et, pour ceux émanant des circuits 17 par un second code, des moyens étant prévus pour qu'au début de la transmission les circuits 11 informent les circuits 17 de leur code et, réciproquement, les circuits 17 informent les circuits 11 de leur code.

Le codage est avantageusement du type polynomial, c'est-à-dire que si le nombre binaire X à coder est de la forme :

$$X = x_n\ x_{n-1} \cdots x_1\ x_o\ ,$$

chaque chiffre binaire du nombre codé a pour valeur :

$$X_p = a_o^p x_o + a_1^p x_1 + \ldots + a_n^p x_n .$$

Dans cette formule, les coefficients a sont des chiffres binaires (0 ou 1) et la variable x_n est un bit du nombre à coder, n étant son poids.

Pour effectuer ce codage, on fait appel (figure 3) à un registre à décalage 50 à entrée série 51, sortie série 52, et dix sorties parallèles, respectivement 53_0 à 53_9 correspondant à chacune des cases de ce registre 50.

A la sortie 53_0 est reliée une entrée 54 d'une porte 55 du type OU exclusif dont l'autre entrée est reliée à la sortie d'une autre porte OU exclusif 56 dont une première entrée 57 est connectée à la sortie 53_5. La seconde entrée de la porte 56 est connectée à la sortie d'une troisième porte OU exclusif 58 dont la première entrée est connectée à la sortie 53_7 et la seconde entrée à la sortie 53_9.

Si, dans cet exemple, le nombre codé est positionné dans le registre de façon telle que le bit x_o soit dans la case de rang 0 et le bit x_9 dans la case de rang 9, le chiffre binaire obtenu sur la sortie 59 de la porte 55 est :

$$X_0 = x_o + x_5 + x_7 + x_9$$

la sortie 52 étant reliée à l'entrée 51, chaque signal d'horloge fait avancer d'un pas le contenu des cases du registre 50, le second bit x_1 du nombre codé apparaissant sur la sortie 59 a alors la valeur :

$$X_1 = x_1 + x_6 + x_8 + x_o$$

Les codes sont variables d'une carte à une autre carte et d'un terminal à un autre terminal. Ils peuvent par exemple être choisis au hasard parmi une infinité (choix aléatoire) ou un grand nombre (choix quasi-aléatoire) de codes, lors de la fabrication des circuits, par un choix aléatoire des connexions entre les portes OU exclusif et les sorties parallèles du registre à décalage 50.

Il est également possible d'effectuer le choix, de façon aléatoire ou quasi-aléatoire, du code au moment de la transaction, après l'introduction de la carte dans le terminal. A cet effet, si le codage est réalisé, comme dans l'exemple décrit en relation avec la figure 3, à l'aide d'un registre

à décalage et de portes du type OU exclusif connectées aux sorties parallèles de ce registre, le choix du code est effectué par l'activation sélective de portes disposées dans les connexions des sorties parallèles du registre à décalage aux entrées des portes OU exclusif. Ces portes sont alternativement ouvertes et fermées à grande vitesse quand la carte et le terminal ne sont pas interconnectés; c'est l'introduction de la carte dans le terminal qui fixe la condition -ouverte ou fermée- de ces portes.

Il est donc impossible à un observateur de connaître au préalable le code ou les codes qui seront utilisés pour la transaction.

Il est bien entendu nécessaire que ces codes soient transmis des circuits 11 aux circuits 17 et vice versa, comme on le verra ci-après en relation avec les figures 4 et 5.

Dans la réalisation représentée sur la figure 4, les circuits 17 du terminal comportent un bloc 65 d'émission-réception dont une borne d'entrée-sortie est reliée à la borne 13_1 et dont une première sortie 66 est connectée à l'entrée 67 d'un décodeur 68 d'un code P_1 qui comprend une sortie 69 reliée à l'entrée d'un registre 70 destiné à mémoriser le code CEN reçu des circuits 11 et qui a été choisi de façon aléatoire ou quasi-aléatoire après introduction de la carte 10 dans le terminal. Le décodeur 68 présente une seconde entrée 71 reliée à la sortie d'un registre 72 dans lequel est stocké le code CAL des circuits 17 qui a été également choisi de façon aléatoire ou quasi-aléatoire après introduction de la carte dans le terminal. La sortie du registre 70 est reliée à une première entrée 73 d'un codeur 74 qui présente une seconde entrée 75 reliée à la sortie du registre 72 ainsi qu'une troisième entrée 76 connectée à la sortie d'un registre 77 contenant l'information confidentielle introduite grâce au clavier 25 par le détenteur de la carte 10.

Le codeur 74 présente une première sortie 78 reliée à une entrée 79 du circuit 65 d'émission-réception, ainsi que des secondes sorties 80 et 81 dont l'une, 80, est reliée à une première entrée d'une porte, ou comparateur, 82, d'identification d'une information ou code P_3 et l'autre, 81, est

connectée également à une première entrée d'une porte ou comparateur 84 d'identification d'une information ou code P_4. Les secondes entrées 83 et 84a des portes 82 et 84 sont reliées à une sortie 85 du circuit 65. Les sorties 86 et 87 des portes, respectivement 82 et 84, délivrent des chiffres binaires. Si la sortie 86 est à"1",la transaction est refusée. Si la sortie 87 est à"1",la transaction est autorisée.

Sur la sortie 78 du codeur 74 apparaît un message qui est une combinaison linéaire des codes appliqués sur ses entrées 73, 75 et 76 ainsi que d'un code P_2 qui est spécifique au terminal. Le message sortant de la borne 80 du codeur 74 est une combinaison linéaire des codes appliqués sur ses entrées 73, 75 et 76 ainsi que d'un code P_3 également spécifique au terminal. Sur la sortie 81 apparaît une combinaison linéaire des messages appliqués sur les entrées 73, 75 et 76 ainsi que d'un autre code P_4 également spécifique au terminal.

Un aiguillage (non montré) est prévu pour que le signal émanant du registre 72 soit appliqué soit sur l'entrée 75 du codeur 74, soit directement sur la ligne E/S.

Les codes P_1 , P_2 , P_3 et P_4 sont des codes inscrits à demeure dans les circuits de la carte et les circuits du terminal. Ils sont identiques dans une série de cartes et de terminaux destinés à effectuer les mêmes opérations. Ces codes ont été choisis au hasard, lors de la fabrication des cartes et des terminaux, parmi une infinité ou un grand nombre de codes.

De façon analogue, les circuits 11 comportent (figure 5) un circuit d'émission-réception 100 présentant une borne d'entrée-sortie reliée à la borne 13, une borne de sortie 101 reliée à l'entrée 102 d'un registre 103 destiné à stocker le code CAL reçu des circuits 17. La sortie du registre 103 est reliée à une entrée 104 d'un codeur 105 cryptant selon le code P_1. Ce codeur 105 présente une seconde entrée 106 reliée à la sortie d'un autre registre 107 dans lequel est mémorisé le code CEN des circuits 11. La sortie du codeur 105 est reliée à une entrée 107' du circuit 100.

Les circuits 11 présentent encore un autre registre 109 dont la sortie est reliée à une entrée 110 d'un comparateur 111a dont l'autre entrée est reliée à la sortie d'un décodeur 111 destiné à décrypter le code P_2.

La sortie du registre 103 est reliée à une entrée 114 du décodeur 111 ainsi qu'à une entrée 115 d'un codeur 113 cryptant selon le code P_3 ou le code P_4 en fonction de la valeur des signaux appliqués sur ses entrées 123 et 124. De façon analogue, la sortie du registre 107 est connectée à une seconde entrée 117 du décodeur 111 et à une seconde entrée 118 du codeur 113. La sortie du décodeur 111 est reliée à une autre entrée 112 du codeur 113 par l'intermédiaire d'un registre 112a destiné à mémoriser l'information en provenance du registre 77 correspondant au code introduit par le détenteur de la carte grâce au clavier 25.

Le décodeur 111 présente une troisième entrée 119 reliée à une sortie 120 du circuit 100.

Le comparateur 111a présente deux sorties connectées à deux mémoires, par exemple des bascules bistables, respectivement 121 pour l'autorisation de transaction et 122 pour le refus de la transaction. Les sorties de ces mémoires 121 et 122 sont connectées aux entrées, respectivement 123 et 124, du codeur 113.

Enfin, ce codeur 113 présente une sortie 125 reliée à une entrée 126 du circuit 100.

Le fonctionnement est le suivant :

Après la phase d'initialisation décrite ci-dessus, le code CAL stocké dans le registre 72 est transmis en clair, c'est-à-dire non codé, sur la ligne E/S. Il est reçu par le circuit 100 qui l'aiguille vers le registre 103 (figure 5).

Ensuite, le codeur 105 transmet une combinaison des code CAL -appliqué sur son entrée 104-, CEN -appliqué sur son entrée 106- et P_1 à l'entrée 107' du circuit 100 et de là au circuit 65 (figure 4) qui l'aiguille vers l'entrée 67 du décodeur 68 recevant sur son autre entrée 71 le code CAL.

La combinaison de codes mentionnée ci-dessus qui est effectuée par le codeur 105 est par exemple une addition. A cet effet, on prévoit (figure 6) un premier codeur 141 analogue à celui représenté sur la figure 3 dont la sortie 140 est reliée à une entrée d'une porte OU exclusif 142 dont la

seconde entrée est reliée à la sortie 143 d'un second codeur 144 également analogue à celui représenté sur la figure 3.

Le message appliqué sur l'entrée 67 du décodeur 68, conçu pour décrypter le code P_1 et sur une entrée 71 duquel est appliqué le code CAL, est décrypté et sur la sortie 69 apparaît le code CEN qui avait été crypté par les codes P_1 et CAL. Ce code CEN est stocké dans le registre 70. Ainsi, à l'issue de cette seconde phase d'échange de messages, le code CEN des circuits de la carte est stocké dans les circuits du terminal et réciproquement le code CAL des circuits du terminal est stocké dans les circuits de la carte.

Après cette seconde phase, le codeur 74 est activé pour que soit appliquée sur l'entrée 79 du circuit 65 une combinaison linéaire des messages appliqués sur les entrées 73, 75 et 76, c'est-à-dire du code CEN, du code CAL et de l'information introduite dans le registre 77 grâce au clavier 25, ainsi que d'un code P_2. Ce message est transmis, par la ligne E/S, au circuit 100 (figure 5) qui l'aiguille sur sa sortie 120, c'est-à-dire à l'entrée 119 du décodeur 111 permettant de décrypter le code P_2 et ladite combinaison linéaire, les codes CAL et CEN étant appliqués sur ses entrées, respectivement 114 et 117. Le signal apparaissant sur la sortie du décodeur 111 est donc l'information qui avait été introduite grâce au clavier 25. Cette dernière information est, d'une part, stockée dans le registre 112a et, d'autre part, comparée grâce au comparateur 111a, à l'information confidentielle que contient le registre 109, le résultat de la comparaison étant mémorisé dans la bascule 121 (autorisation de transaction) ou dans la bascule 122 (refus de transaction).

Selon une disposition importante de l'invention, ces informations d'autorisation ou de refus ne sont pas transmises en clair sur la ligne E/S mais sont codées de façon complexe à l'aide du codeur 113. Le but de ce dernier est de transformer l'information binaire d'autorisation en un code ou information complexe P_3 crypté par le code CAL, le code CEN et l'information ou code du registre 112a. En cas de refus, c'est-à-dire si un "1" est appliqué sur l'entrée 124 du codeur 113, ce dernier transforme l'information binaire de refus en un

code complexe P_4 crypté par les informations fournies par les registres 103, 107 et 112a. Les informations ou codes P_3 et P_4 ont des compositions ou structures très voisines de façon que leur analyse, dans une intention frauduleuse, soit rendue très difficile. Le message provenant de la sortie du codeur 113 est ainsi transmis au circuit 65 d'où il est aiguillé, par la sortie 85 de ce dernier, vers les entrées 83 et 84a des comparateurs 82 et 84. Le comparateur 82 reçoit, par son autre entrée connectée à la sortie 80 du codeur 74, une information qui est une combinaison linéaire des codes CEN, CAL, du code mémorisé dans le registre 77, et du code P_3 engendré par le codeur 74. Si cette information est identique à celle reçue sur l'entrée 83, sur la sortie 86 est alors émis un signal "1" représentant l'autorisation. Sur la sortie 81 du codeur 74 est engendré un signal qui est une combinaison des messages appliqués sur ses entrées 73, 75 et 76 ainsi que du code P_4. Si l'information provenant de la carte est un refus, il apparaîtra ainsi un signal "1" sur la sortie 87.

L'information stockée dans la mémoire 77 est soit inscrite en clair, soit cryptée selon P_2 pour augmenter encore la difficulté de la fraude.

REVENDICATIONS

1.- Système comprenant un objet portatif, à circuits intégrés électroniques portant une information confidentielle, et un lecteur dans lequel peut être introduit ledit objet afin de déclencher une opération telle qu'une transaction, caractérisé en ce que les circuits électroniques intégrés de l'objet et du lecteur sont spécifiques, non programmables, de façon que la durée d'échange des signaux entre les circuits de l'objet et ceux du lecteur soit réduite à un minimum, et en ce que des moyens sont prévus pour interdire l'opération si le temps d'exécution des échanges dépasse une limite prédéterminée.

2.- Système selon la revendication 1, caractérisé en ce qu'il comporte un circuit de demandes de répétition de message lorsqu'un message reçu par le circuit de la carte et/ou du lecteur ne correspond pas à des conditions prédéterminées, un compteur de ces demandes de répétition, et un moyen pour interdire l'opération si le nombre de demandes de répétion dépasse un nombre déterminé N.

3.- Système selon la revendication 2, caractérisé en ce que le nombre N est inférieur au nombre total de messages à échanger entre les circuits de l'objet et ceux du lecteur.

4.- Système selon la revendication 2 ou la revendication 3, caractérisé en ce que le nombre N est au moins égal à deux.

5.- Système comprenant un objet portatif à circuits intégrés électroniques portant une information confidentielle et un lecteur dans lequel peut être introduit ledit objet afin de déclencher une opération telle qu'une transaction, caractérisé en ce que les circuits de l'objet et/ou du lecteur présentent un moyen de codage des messages à transmettre à l'autre partie du système, et en ce que des moyens sont prévus pour transmettre le code à ladite autre partie.

6.- Système selon la revendication 5, caractérisé en ce que le code est choisi au hasard parmi un grand nombre ou une infinité de codes lors de la fabrication du circuit qui le comporte.

7.- Système selon la revendication 5, caractérisé en ce que le code est choisi au hasard parmi un grand nombre ou

une infinité de codes lors de l'introduction de l'objet dans le lecteur.

8.- Système selon l'une quelconque des revendications 5 à 7, caractérisé en ce que le moyen de codage comporte un registre à décalage à entrée série, un chiffre du nombre codé étant une combinaison prédéterminée des chiffres apparaissant sur les sorties parallèles du registre.

9.- Système selon la revendication 8, caractérisé en ce que la combinaison prédéterminée est une opération d'addition.

10.- Système selon la revendication 9, caractérisé en ce que l'addition est réalisée par une (ou plusieurs) porte(s) du type OU exclusif.

11.- Système selon l'une quelconque des revendications 5 à 10, caractérisé en ce que des messages émis par les circuits de l'objet vers ceux du lecteur ou vice versa sont codés suivant une combinaison d'un code propre à ce circuit et d'un code provenant de l'autre partie du système.

12.- Système comprenant un objet portatif à circuits intégrés électroniques présentant une information confidentielle et un lecteur dans lequel peut être introduit ledit objet afin de déclencher une opération telle qu'une transaction et comportant un moyen tel qu'un clavier pour que le détenteur de l'objet mémorise une information, en principe identique à l'information confidentielle, et des moyens sont prévus pour comparer les deux informations afin d'autoriser ou non, selon le résultat de la comparaison, le déclenchement de l'opération, caractérisé en ce que, la comparaison étant effectuée dans les circuits de l'objet et son résultat (autorisation ou refus) transmis aux circuits du lecteur, les circuits de l'objet comportent des moyens de cryptage tels que l'autorisation et le refus sont représentés par des messages, transmis aux circuits du lecteur, ayant des structures très voisines, le décryptage étant effectué dans les circuits du lecteur.

13.- Objet portatif pour système selon l'une quelconque des revendications précédentes.

14.- Lecteur pour système selon l'une quelconque des revendications 1 à 12.

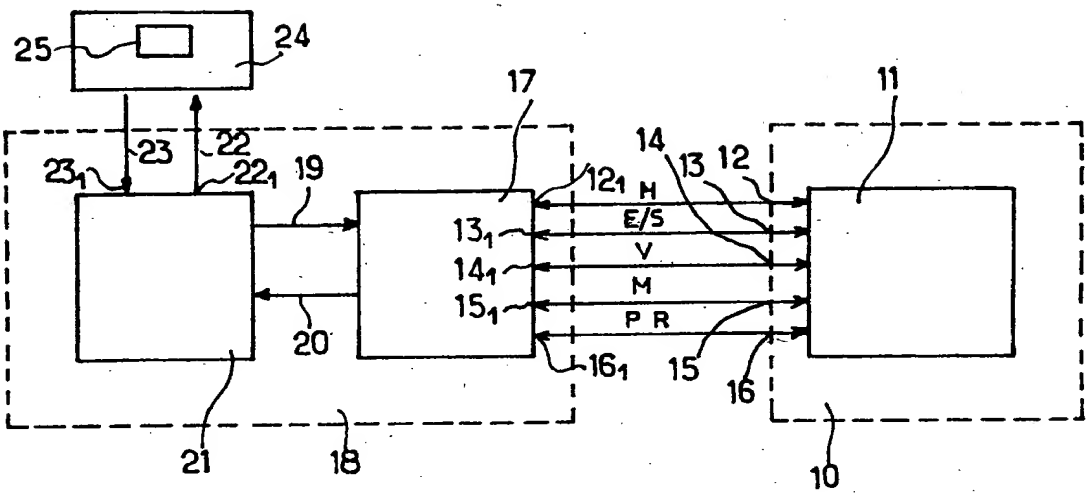
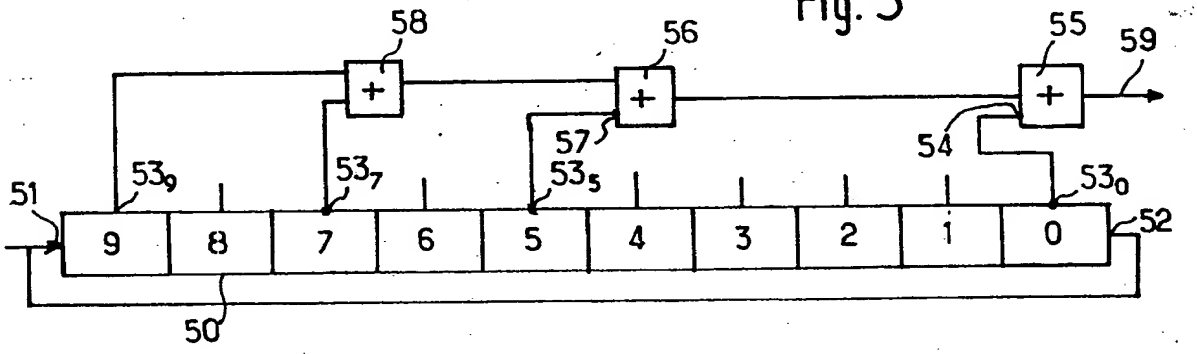


Fig. 1

Fig. 3



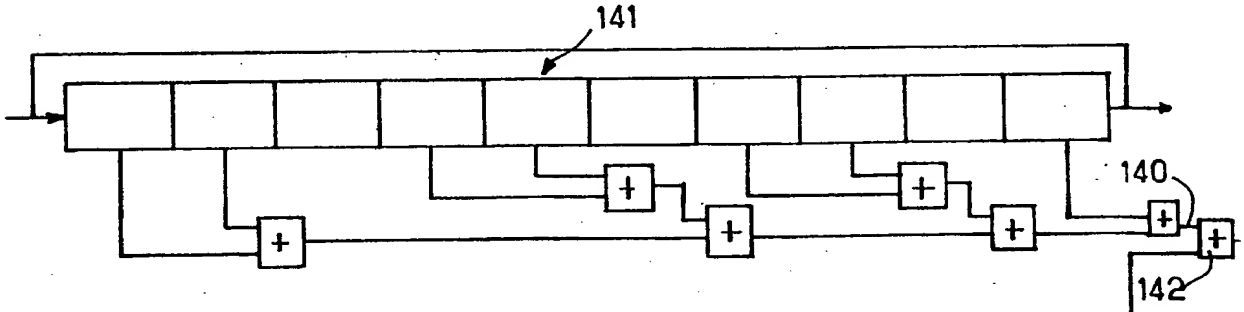


Fig. 6

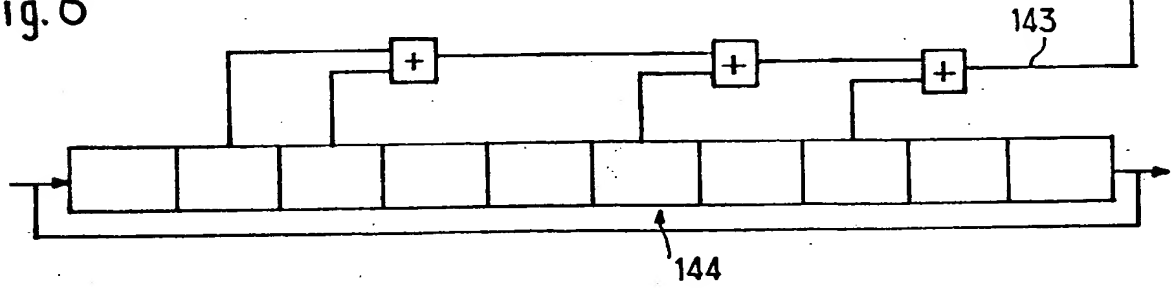


Fig.2

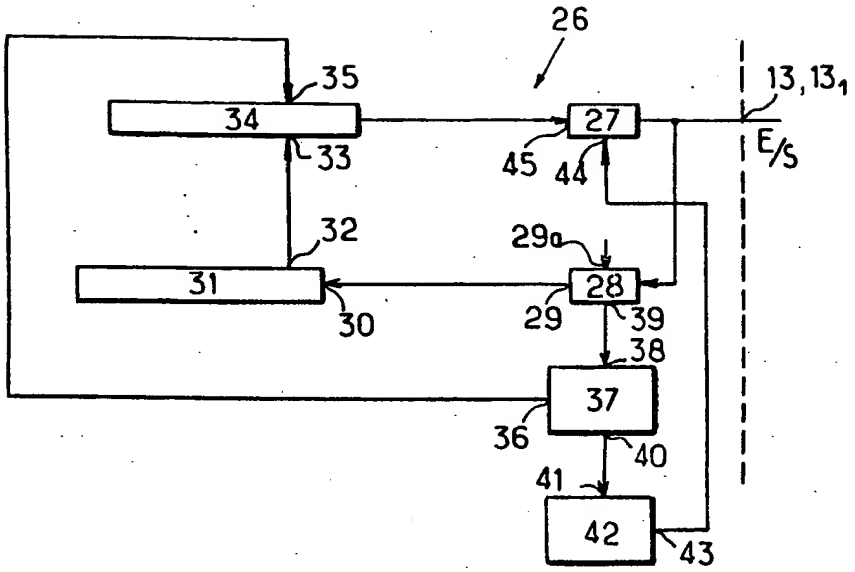
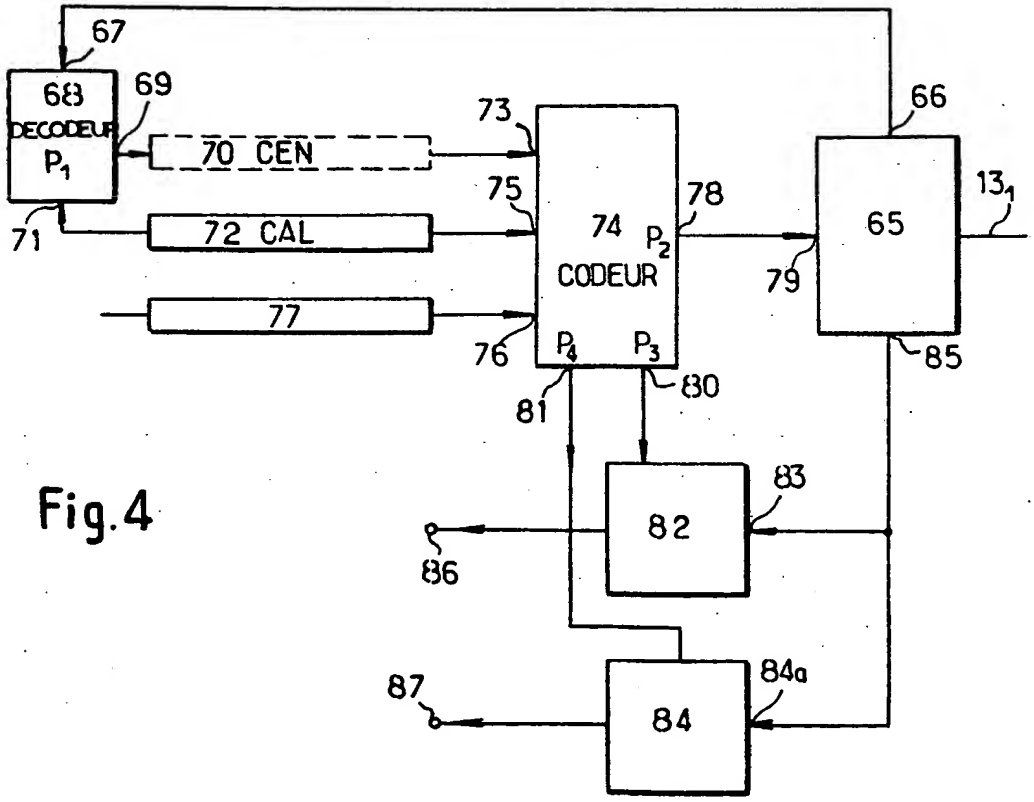

26
35
34
33
27
13, 13₁
E/S
45
44
32
29a
31
30
28
29
39
38
37
36
40
41
42
43

Fig.4


67
68
DECODEUR
P1
69
70 CEN
71
72 CAL
73
75
74
CODEUR
P2
78
66
65
13₁
79
77
76
P4
P3
80
85
81
82
83
86
87
84
84a

2471003

Fig.5